

Isomorphic tetravalent cyclic Haar graphs

S. Hiroki Koike-Quintanar*

University of Primorska, UP IAM
Muzejski trg 2, SI6000 Koper, Slovenia

hiroki.koike@upr.si

István Kovács†

University of Primorska, UP IAM and UP FAMNIT
Muzejski trg 2, SI6000 Koper, Slovenia

istvan.kovacs@upr.si

December 14, 2012

Abstract

Let S be a subset of the cyclic group \mathbb{Z}_n . The cyclic Haar graph $H(\mathbb{Z}_n, S)$ is the bipartite graph with color classes \mathbb{Z}_n^+ and \mathbb{Z}_n^- , and edges $\{x^+, y^-\}$, where $x, y \in \mathbb{Z}_n$ and $y - x \in S$. In this paper we give sufficient and necessary conditions for the isomorphism of two connected cyclic Haar graphs of valency 4.

Keywords: graph isomorphism, cyclic Haar graph, 4-BCI-group.

MSC 2010: 20B25, 05C25, 05C60.

1 Introduction

Let S be a subset of a finite group G . The *Haar graph* $H(G, S)$ is the bipartite graph with color classes identified with G and written as G^+ and G^- , and the edges are $\{x^+, y^-\}$, where $x, y \in G$ and $yx^{-1} \in S$. Haar graphs were introduced for abelian groups by Hladnik, Marušič and Pisanski [6], and were redefined under the name *bi-Cayley graphs* in [17]. A Haar graph $H(G, S)$ is called *cyclic* if G is a cyclic group. In this paper we consider the problem of giving sufficient and necessary conditions for the isomorphism of two cyclic Haar graphs. This is a natural continuation of the isomorphism problem of circulant digraphs which has been solved by Muzychuk [12]. It appears in the context of circulant matrices under the name bipartite Ádám problem [16], and also in the context of cyclic configurations [2, 6].

*Supported in part by ARRS – Agencija za raziskovanje Republike Slovenije, program no. P1-0285.

†Supported in part by ARRS – Agencija za raziskovanje Republike Slovenije, program no. P1-0285.

The symbol \mathbb{Z}_n denotes the additive group of the ring $\mathbb{Z}/n\mathbb{Z}$ of residue classes modulo n , and \mathbb{Z}_n^* denotes the multiplicative group of units in $\mathbb{Z}/n\mathbb{Z}$. Two Haar graphs $H(\mathbb{Z}_n, S)$ and $H(\mathbb{Z}_n, T)$ are called *affinely equivalent*, written as $H(\mathbb{Z}_n, S) \cong_{\text{aff}} H(\mathbb{Z}_n, T)$, if S can be mapped to T by an affine transformation, i.e., $aS + b = T$ for some $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n$. It is an easy exercise to show that two affinely equivalent cyclic Haar graphs are isomorphic as usual graphs. The converse implication is not true in general, and this makes the following definition interesting (see [17]): we say that a subset $S \subseteq \mathbb{Z}_n$ is a *BCI-subset* if for each $T \subseteq G$, $H(\mathbb{Z}_n, S) \cong H(\mathbb{Z}_n, T)$ if and only if $H(\mathbb{Z}_n, S) \cong_{\text{aff}} H(\mathbb{Z}_n, T)$. Wiedemann and Zieve proved in [16, Theorem 1.1] that any subset S of \mathbb{Z}_n is a BCI-subset if $|S| \leq 3$ (a special case was proved earlier in [3]). However, this is not true if $|S| \geq 4$ (see [6, 16]), hence the first nontrivial case of the isomorphism problem occurs when $|S| = 4$. In this paper we settle this case by proving the following theorem:

Theorem 1.1. *Two connected Haar graphs $H(\mathbb{Z}_n, S)$ and $H(\mathbb{Z}_n, T)$ with $|S| = |T| = 4$ are isomorphic if and only if there exist $a_1, a_2 \in \mathbb{Z}_n^*$ and $b_1, b_2 \in \mathbb{Z}_n$ such that*

- (1) $a_1S + b_1 = T$; or
- (2) $a_1S + b_1 = \{0, u, v, v + m\}$ and $a_2T + b_2 = \{0, u + m, v, v + m\}$, where $n = 2m$, $\mathbb{Z}_n = \langle u, v \rangle$, $2 \mid u$, $2u \mid m$ and $u/2 \not\equiv v + m/(2u) \pmod{m/u}$.

Remark. A group G is called an *m-BCI-group* if every subset S of G with $|S| \leq m$ is a BCI-subset (see [7, 17]). In this context [16, Theorem 1.1] can be rephrased as \mathbb{Z}_n is a 3-BCI-group for any number n ; and Theorem 1.1 says that \mathbb{Z}_n is not a 4-BCI-group if and only if n is divisible by 8. This refines [16, Theorem 7.2] in which it is proved that, if \mathbb{Z}_n contains a non-BCI-subset of size k , $k \in \{4, 5\}$, then n has a prime divisor less or equal to $2k(k - 1)$.

Our approach is group theoretical, we adopt the ideas of [1, 11]. In short terms the initial problem is transformed to a problem about the automorphism group of the graphs in question. Theorem 1.1 is proven in two steps: first it is settled for graphs $H(\mathbb{Z}_n, S)$ with S satisfying additional conditions (see Theorem 3.1); then it is shown that, if S is not a BCI-subset, then it is affinely equivalent to a set satisfying the conditions of Theorem 3.1 (see Theorem 4.1).

2 A Babai type theorem

In this paper every group, graph and digraph is finite. For a (di)graph Γ , the symbols $V(\Gamma)$, $E(\Gamma)$ and $\text{Aut}(\Gamma)$ denote the set of its vertices, (directed) edges and the full group of its automorphisms, respectively. Regarding terminology and notation in permutation group theory we follow [5].

Let S be a subset of a group G . The *Cayley digraph* $\text{Cay}(G, S)$ is the digraph with vertex set G , and its directed edges are (x, y) , where $x, y \in G$ and $yx^{-1} \in S$. Two digraphs $\text{Cay}(G, S)$ and $\text{Cay}(G, T)$ are called *Cayley isomorphic*, written as $\text{Cay}(G, S) \cong_{\text{cay}} \text{Cay}(G, T)$, if $T = S^\varphi$ for some group automorphism $\varphi \in \text{Aut}(G)$. It is clear that such

an automorphism induces an isomorphism between $\text{Cay}(G, S)$ and $\text{Cay}(G, T)$, and thus Cayley isomorphic digraphs are isomorphic as usual digraphs. It is also well-known that the converse implication is not true, and this makes sense for the following definition (see [1]): a subset $S \subseteq G$ is a *CI-subset* if for each $T \subseteq G$, $\text{Cay}(G, S) \cong \text{Cay}(G, T)$ if and only if $\text{Cay}(G, S) \cong_{\text{cay}} \text{Cay}(G, T)$. The following equivalence was proved by Babai [1, 3.1 Lemma].

Theorem 2.1. *The following are equivalent for every Cayley digraph $\text{Cay}(G, S)$.*

- (1) *S is a CI-subset.*
- (2) *Every two regular subgroups of $\text{Aut}(\text{Cay}(G, S))$ isomorphic to G are conjugate in $\text{Aut}(\text{Cay}(G, S))$.*

Theorem 2.1 essentially says that the CI-property of a given subset S depends entirely on the automorphism group $\text{Aut}(\text{Cay}(G, S))$. In this section we prove analogous results for cyclic Haar graphs.

Let $V = V(H(\mathbb{Z}_n, S))$ be the vertex set of the Haar Graph $H(\mathbb{Z}_n, S)$. Throughout this paper c and d denote the permutations of V defined by

$$c : x^\varepsilon \mapsto (x + 1)^\varepsilon \text{ and } d : x^\varepsilon \mapsto \begin{cases} (n - x)^- & \text{if } \varepsilon = +, \\ (n - x)^+ & \text{if } \varepsilon = -, \end{cases} \quad (1)$$

where $x \in \mathbb{Z}_n$ and $\varepsilon \in \{+, -\}$. It follows immediately that both c and d are automorphisms of any Haar graph $H(\mathbb{Z}_n, S)$. Denote by C the group generated by c , and by D the group generated by c and d . The group D acts regularly on V , and D is isomorphic to D_{2n} . Thus $H(\mathbb{Z}_n, S)$ is isomorphic to a Cayley graph over D , and so Theorem 2.1 can be applied. The following corollary is obtained.

Corollary 2.2. *The implication (1) \Leftarrow (2) holds for every Haar graph $H(\mathbb{Z}_n, S)$.*

- (1) *S is a BCI-subset.*
- (2) *Every two regular subgroups of $\text{Aut}(H(\mathbb{Z}_n, S))$ isomorphic to D are conjugate in $\text{Aut}(H(\mathbb{Z}_n, S))$.*

However, we do not have equivalence in Corollary 2.2 as it is shown in the following example.

Example 2.3. Let $\Gamma = H(\mathbb{Z}_{10}, \{0, 1, 3, 4\})$. Using the computer package MAGMA [4] we compute that Γ is edge-transitive and its automorphism group $\text{Aut}(\Gamma) \cong D_{20} \rtimes \mathbb{Z}_4$. Furthermore, $\text{Aut}(\Gamma)$ contains a regular subgroup X which is isomorphic to D_{20} but $X \neq D_{20}$, hence (2) in Corollary 2.2 does not hold.

On the other hand, we find that for every subset $T \subseteq \mathbb{Z}_{10}$ with $0 \in T$ and $|T| = 4$, the corresponding Haar graph $H(\mathbb{Z}_{10}, T) \cong \Gamma$ exactly when $H(\mathbb{Z}_{10}, T) \cong_{\text{aff}} \Gamma$. Thus $\{0, 1, 3, 4\}$ is a BCI-subset, so (1) in Corollary 2.2 is true. ■

Example 2.3 shows that the isomorphism problem of cyclic Haar graphs is not a particular case of the isomorphism problem of Cayley graphs over dihedral groups. We remark that the latter problem is still unsolved, for partial solutions, see [1, 13, 14]. Nonetheless, the idea of Babai works well if instead of the regular subgroup D we consider its index 2 cyclic subgroup C .

We say that a permutation group $G \leq \text{Sym}(\mathbb{Z}_n^+ \cup \mathbb{Z}_n^-)$ is *bicyclic* if G is a cyclic group which has two orbits: \mathbb{Z}_n^+ and \mathbb{Z}_n^- . By a bicyclic group of a Haar graph $\Gamma = H(\mathbb{Z}_n, S)$ we simply mean a bicyclic subgroup $X \leq \text{Aut}(\Gamma)$. Obviously, C is a bicyclic group of any cyclic Haar graph, and being so it will be referred to as the *canonical bicyclic group*.

Let $\text{Iso}(\Gamma)$ denote the set of all isomorphisms from Γ to any other Haar graph $H(\mathbb{Z}_n, T)$, i.e.,

$$\text{Iso}(\Gamma) = \{f \in \text{Sym}(V) : \Gamma^f = H(\mathbb{Z}_n, T) \text{ for some } T \subseteq \mathbb{Z}_n\}.$$

And let $\mathcal{C}_{\text{iso}}(\Gamma)$ denote the *isomorphism class* of cyclic Haar graphs which contains Γ , i.e., $\mathcal{C}_{\text{iso}}(\Gamma) = \{\Gamma^f : f \in \text{Iso}(\Gamma)\}$.

Lemma 2.4. *Let $\Gamma = H(\mathbb{Z}_n, S)$ be a connected Haar graph and f be in $\text{Sym}(V)$. Then $f \in \text{Iso}(\Gamma)$ if and only if fCf^{-1} is a bicyclic group of Γ .*

PROOF. Let $f \in \text{Iso}(\Gamma)$. Then $fCf^{-1} \leq \text{Aut}(\Gamma)$. Clearly, fCf^{-1} is a cyclic group. Since the sets \mathbb{Z}_n^+ and \mathbb{Z}_n^- are the color classes of the connected bipartite graph Γ , f preserves these color classes, implying that $\text{Orb}(fCf^{-1}, V) = \{\mathbb{Z}_n^+, \mathbb{Z}_n^-\}$. The group fCf^{-1} is a bicyclic group of Γ .

Conversely, suppose that fCf^{-1} is a bicyclic group of Γ . Then $C = f^{-1}(fCf^{-1})f \leq \text{Aut}(\Gamma^f)$. Because that $\text{Orb}(fCf^{-1}, V) = \{\mathbb{Z}_n^+, \mathbb{Z}_n^-\}$, the graph Γ^f is connected and bipartite with color classes \mathbb{Z}_n^+ and \mathbb{Z}_n^- . We conclude that $\Gamma^f = H(\mathbb{Z}_n, T)$ for some $T \subseteq \mathbb{Z}_n$, so $f \in \text{Iso}(\Gamma)$. The lemma is proved. ■

Lemma 2.4 shows that the normalizer $N_{\text{Sym}(V)}(C) \subseteq \text{Iso}(H(\mathbb{Z}_n, S))$. The group $N_{\text{Sym}(V)}(C)$ is known to consist of the following permutations:

$$\varphi_{r,s,t} : x^\varepsilon \mapsto \begin{cases} (rx + s)^+ & \text{if } \varepsilon = +, \\ (rx + t)^- & \text{if } \varepsilon = -, \end{cases} \quad \psi_{r,s,t} : x^\varepsilon \mapsto \begin{cases} (rx + s)^- & \text{if } \varepsilon = +, \\ (rx + t)^+ & \text{if } \varepsilon = -, \end{cases} \quad (2)$$

where $r \in \mathbb{Z}_n^*$ and $s, t \in \mathbb{Z}_n$. Note that, two Haar graphs $H(\mathbb{Z}_n, S)$ and $H(\mathbb{Z}_n, T)$ are from the same orbit under $N_{\text{Sym}(V)}(C)$ exactly when $H(\mathbb{Z}_n, S) \cong_{\text{aff}} H(\mathbb{Z}_n, T)$. Let $\mathcal{C}_{\text{aff}}(\Gamma)$ denote the *affine equivalence class* of cyclic Haar graphs which contains the graph $\Gamma = H(\mathbb{Z}_n, S)$, i.e., $\mathcal{C}_{\text{aff}}(\Gamma) = \{\Gamma^\varphi : \varphi \in N_{\text{Sym}(V)}(C)\}$. It is clear that the isomorphism class $\mathcal{C}_{\text{iso}}(\Gamma)$ splits into affine equivalence classes:

$$\mathcal{C}_{\text{iso}}(\Gamma) = \mathcal{C}_{\text{aff}}(\Gamma_1) \dot{\cup} \cdots \dot{\cup} \mathcal{C}_{\text{aff}}(\Gamma_k)^1.$$

Our next goal is to describe the above decomposition with the aid of bicyclic groups. Let X be a bicyclic group of a connected graph $\Gamma = H(\mathbb{Z}_n, S)$. Then $g^{-1}Xg$ is also a

¹Here we mean that $\mathcal{C}_{\text{iso}}(\Gamma) = \mathcal{C}_{\text{aff}}(\Gamma_1) \cup \cdots \cup \mathcal{C}_{\text{aff}}(\Gamma_k)$ and $\mathcal{C}_{\text{aff}}(\Gamma_i) \cap \mathcal{C}_{\text{aff}}(\Gamma_j) = \emptyset$ for every $i, j \in \{1, \dots, k\}$, $i \neq j$.

bicyclic group for every $g \in \text{Aut}(\Gamma)$, hence the full set of bicyclic groups of Γ is the union of $\text{Aut}(\Gamma)$ -conjugacy classes. We say that a subset $\Xi \subseteq \text{Iso}(\Gamma)$ is a *bicyclic base* of Γ if the subgroups $\xi C \xi^{-1}$, $\xi \in \Xi$, form a complete set of representatives of the corresponding conjugacy classes. Thus every bicyclic group X can be expressed as

$$X = g \xi C (g \xi)^{-1} \text{ for a unique } \xi \in \Xi \text{ and } g \in \text{Aut}(\Gamma).$$

Remark. Our definition of a bicyclic base copies in a sense the definition of a cyclic base introduced by Muzychuk [11, Definition, page 591].

Theorem 2.5. *Let $\Gamma = H(\mathbb{Z}_n, S)$ be a connected Haar graph with a bicyclic base Ξ . Then $\mathcal{C}_{\text{iso}}(\Gamma) = \bigcup_{\xi \in \Xi} \mathcal{C}_{\text{aff}}(\Gamma^\xi)$.*

PROOF. It follows immediately that,

$$\mathcal{C}_{\text{iso}}(\Gamma) \supseteq \bigcup_{\xi \in \Xi} \mathcal{C}_{\text{aff}}(\Gamma^\xi). \quad (3)$$

We prove that equality holds in (3). Pick $\Sigma \in \mathcal{C}_{\text{iso}}(\Gamma)$. Then $\Sigma = \Gamma^f$ for some $f \in \text{Iso}(\Gamma)$. By Lemma 2.4, $f C f^{-1}$ is a bicyclic group of Γ , hence

$$f C f^{-1} = g \xi C (g \xi)^{-1}, \quad \xi \in \Xi, g \in \text{Aut}(\Gamma).$$

Thus $f^{-1} g \xi = h$, where $h \in N_{\text{Sym}(V)}(C)$. Then

$$\Sigma = \Gamma^f = \Gamma^{g \xi h^{-1}} = (\Gamma^\xi)^{h^{-1}}.$$

This shows that $\Sigma \in \mathcal{C}_{\text{aff}}(\Gamma^\xi)$, and so

$$\mathcal{C}_{\text{iso}}(\Gamma) \subseteq \bigcup_{\xi \in \Xi} \mathcal{C}_{\text{aff}}(\Gamma^\xi).$$

In view of (3) the two sides are equal.

Moreover, if $\Sigma \in \mathcal{C}_{\text{aff}}(\Gamma^{\xi_1}) \cap \mathcal{C}_{\text{aff}}(\Gamma^{\xi_2})$ for $\xi_1, \xi_2 \in \Xi$, then $\Gamma^{\xi_1} = \Gamma^{\xi_2 h}$ for some $h \in N_{\text{Sym}(V)}(C)$. Hence $\xi_2 h \xi_1^{-1} = g$ for some $g \in \text{Aut}(\Gamma)$, and so

$$\xi_1 C \xi_1^{-1} = g^{-1} \xi_2 h C h^{-1} \xi_2^{-1} g = g^{-1} (\xi_2 C \xi_2^{-1}) g.$$

The bicyclic subgroups $\xi_1 C \xi_1^{-1}$ and $\xi_2 C \xi_2^{-1}$ are conjugate in $\text{Aut}(\Gamma)$, hence $\xi_1 = \xi_2$ follows from the definition of the bicyclic base Ξ . We obtain that $\mathcal{C}_{\text{aff}}(\Gamma^{\xi_1}) \cap \mathcal{C}_{\text{aff}}(\Gamma^{\xi_2}) = \emptyset$ whenever $\xi_1, \xi_2 \in \Xi$, $\xi_1 \neq \xi_2$, and so $\mathcal{C}_{\text{iso}}(\Gamma) = \bigcup_{\xi \in \Xi} \mathcal{C}_{\text{aff}}(\Gamma^\xi)$. The theorem is proved. \blacksquare

As a direct consequence of Theorem 2.5 we obtain the following corollary, analog of Theorem 2.1.

Corollary 2.6. *The following are equivalent for every connected Haar graph $H(\mathbb{Z}_n, S)$.*

(1) S is a BCI-subset.

(2) Any two bicyclic groups of $H(\mathbb{Z}_n, S)$ are conjugate in $\text{Aut}(H(\mathbb{Z}_n, S))$.

In our last proposition we connect the BCI-property with the CI-property. For $a^\varepsilon \in V$, in what follows $\text{Aut}(H(\mathbb{Z}_n, S))_{a^\varepsilon}$ denotes the vertex stabilizer of a^ε in $\text{Aut}(H(\mathbb{Z}_n, S))$.

Proposition 2.7. *Suppose that $\Gamma = H(\mathbb{Z}_n, S)$ is a connected Haar graph such that $\text{Aut}(\Gamma)_{0^+} = \text{Aut}(\Gamma)_{a^-}$ for some $a \in \mathbb{Z}_n$. Then the following are equivalent.*

(1) S is a BCI-subset.

(2) $S - a = \{s - a : s \in S\}$ is a CI-subset.

PROOF. For sake of simplicity we put $A = \text{Aut}(\Gamma)$ and G for the setwise stabilizer $\text{Aut}(\Gamma)_{\{\mathbb{Z}_n^+\}}$ of the color class \mathbb{Z}_n^+ in $\text{Aut}(\Gamma)$. Obviously, $X \leq G$ for every bicyclic group X of Γ . Since $A = G \rtimes \langle d \rangle$ and d normalizes C , it follows that the conjugacy class of subgroups of A containing C is equal to the conjugacy class of subgroups of G containing C . Using this and Theorem 2.5, we obtain that S is a BCI-subset if and only if every bicyclic group is conjugate to C in G .

Let $W = \{0^+, a^-\}$ and consider the setwise stabilizer $A_{\{W\}}$. Since $A_{0^+} = A_{a^-}$, $A_{0^+} \leq A_{\{W\}}$. By [5, Theorem 1.5A], the orbit of 0^+ under $A_{\{W\}}$ is a block of imprimitivity (for short a block) for A . Denote this block by Δ and the induced system of blocks by δ (i.e., $\delta = \{\Delta^g : g \in G\}$). Consider the element $g = dc^a$ from D . We see that g switches 0^+ and a^- , hence $A_{\{W\}} = A_{0^+} \langle g \rangle$. Therefore, $\Delta = (0^+)^{A_{\{W\}}} = (0^+)^{A_{0^+} \langle g \rangle} = (0^+)^{\langle g \rangle} = W$, and so

$$\delta = \{ \{x^+, (x+a)^-\} : x \in \mathbb{Z}_n \}.$$

Define the mapping $\varphi : \delta \rightarrow \mathbb{Z}_n$ by $\varphi : \{x^+, (x+a)^-\} \mapsto x$, $x \in \mathbb{Z}_n$. Now, an action of A on \mathbb{Z}_n can be defined by letting $g \in A$ act as

$$x^g = x^{\varphi^{-1}g\varphi}, \quad x \in \mathbb{Z}_n.$$

For $g \in A$ we write \bar{g} for the image of g under the corresponding permutation representation, and for a subgroup $X \leq A$ we let $\bar{X} = \{\bar{x} : x \in X\}$. In this action of A the subgroup $G < A$ is faithful. Also notice that, a subgroup $X \leq G$ is a bicyclic group of Γ if and only if \bar{X} is a regular cyclic subgroup of \bar{G} . In particular, for the canonical bicyclic group C , $\bar{C} = (\mathbb{Z}_n)_{\text{right}}$, where $(\mathbb{Z}_n)_{\text{right}}$ denotes the group generated by the affine transformation $x \mapsto x + 1$, $x \in \mathbb{Z}_n$.

Pick $g \in G$ and $(x, x + s - a) \in \mathbb{Z}_n \times \mathbb{Z}_n$, where $s \in S$. Then g maps the directed edge $(x^+, (x+s)^-)$ to a directed edge $(y^+, (y+q)^-)$ for some $y \in \mathbb{Z}_n$ and $q \in S$. Since δ is a system of blocks for G , g maps $(x+s-a)^+$ to $(y+q-a)^+$, and so \bar{g} maps the pair $(x, x+s-a)$ to the pair $(y, y+q-a)$. We have just proved that \bar{g} leaves the set $\{(x, x+s-a) : x \in \mathbb{Z}_n, s \in S\}$ fixed. As the latter set is the set of all directed edges of the digraph $\text{Cay}(\mathbb{Z}_n, S-a)$, $\bar{G} \leq \text{Aut}(\text{Cay}(\mathbb{Z}_n, S-a))$. For an automorphism h of $\text{Cay}(\mathbb{Z}_n, S-a)$, define the permutation g of V by

$$g : x^\varepsilon \mapsto \begin{cases} (x^h)^+ & \text{if } \varepsilon = +, \\ ((x-a)^h + a)^- & \text{if } \varepsilon = -, \end{cases} \quad x \in \mathbb{Z}_n, \varepsilon \in \{+, -\}.$$

The reader is invited to check that the above permutation g is an automorphism of Γ . It is clear that $g \in G$ and $\bar{g} = h$; we conclude that $\bar{G} = \text{Aut}(\text{Cay}(\mathbb{Z}_n, S - a))$.

Now, the proposition follows along the following equivalences:

- (1) \iff Every bicyclic group of Γ is conjugate to C in G
- \iff Every regular cyclic subgroup of \bar{G} is conjugate to \bar{C} in \bar{G}
- \iff (2).

The last equivalence is Theorem 2.1. ■

Remark. We want to remark that the equality $\text{Aut}(\Gamma)_{0+} = \text{Aut}(\Gamma)_{a-}$ does not hold in general. For example, take Γ as the incidence graph of the projective space $\text{PG}(d, q)$ where $d \geq 2$ and q is a prime power (i.e., Γ is the bipartite graph with color classes identified by the points and the hyperplanes, respectively, and the edges are defined by the incidence relation of the space). It is well-known that the space $\text{PG}(d, q)$ admits a cyclic group of automorphisms (called a Singer subgroup) acting regularly on the points and the hyperplanes, respectively. This shows that Γ is isomorphic to a cyclic Haar graph, and we may identify the set of points with \mathbb{Z}_n^+ , and the set of hyperplanes with \mathbb{Z}_n^- , where $n = (q^d - 1)/(q - 1)$. The automorphism group $\text{Aut}(\Gamma) = \text{P}\Gamma\text{L}(d + 1, q) \rtimes \mathbb{Z}_2$. As $\text{P}\Gamma\text{L}(d + 1, q)$ acts inequivalently on the points and the hyperplanes, $\text{Aut}(\Gamma)_{0+}$ cannot be equal to $\text{Aut}(\Gamma)_{a-}$ for any $a \in \mathbb{Z}_n$.

3 Haar graphs $H(\mathbb{Z}_{2m}, \{0, u, v, v + m\})$

In this section we prove Theorem 1.1 for Haar graphs $H(\mathbb{Z}_n, S)$ satisfying certain additional conditions.

Theorem 3.1. *Let $n = 2m$ and $S = \{0, u, v, v + m\}$ such that*

- (a) $\mathbb{Z}_n = \langle u, v \rangle$;
- (b) $1 < u < m, u \mid m$;
- (c) $\text{Aut}(H(\mathbb{Z}_n, S))_{0+}$ leaves the set $\{0^-, u^-\}$ setwise fixed.

Then $H(\mathbb{Z}_n, S) \cong H(\mathbb{Z}_n, T)$ if and only if there exist $a \in \mathbb{Z}_n^$ and $b \in \mathbb{Z}_n$ such that*

- (1) $aT + b = S$; or
- (2) $aT + b = \{0, u + m, v, v + m\}$, and $2 \mid u, 2u \mid m, u/2 \not\equiv v + m/(2u) \pmod{m/u}$.

By (b) of Theorem 3.1 we have $2u \leq m$. We prove the extremal case, when $2u = m$, separately. Notice that, in this case the conditions in (2) of Theorem 3.1 that $2 \mid u, 2u \mid m$ and $u/2 \not\equiv v + m/(2u) \pmod{m/u}$ can be replaced by one condition: $u \equiv 2 \pmod{4}$.

Lemma 3.2. *Let S be the set defined in Theorem 3.1. If $2u = m$, then $H(\mathbb{Z}_n, S) \cong H(\mathbb{Z}_n, T)$ if and only if there exist $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n$ such that*

(1) $aT + b = S$; or

(2) $aT + b = \{0, u + m, v, v + m\}$ and $u \equiv 2 \pmod{4}$.

PROOF. Let $d = \gcd(n, v)$. Because of $\langle u, v \rangle = \mathbb{Z}_n$ we have that $\gcd(u, v, n) = 1$, i.e., $\gcd(n/4, v) = 1$, and this gives that $d \in \{1, 2, 4\}$. Note that, if $d \neq 1$, then necessarily $2 \nmid u$. Then we can write $v = v_1 d$, where $\gcd(v_1, n) = 1$. Let v_1^{-1} denote the inverse of v_1 in the group \mathbb{Z}_n^* . Then the following hold in \mathbb{Z}_n (here use that $u = n/4$):

$$v_1^{-1}v = d, \quad v_1^{-1}(v + 2u) = d + 2u \quad \text{and} \quad v_1^{-1}u \in \{u, 3u\}.$$

We conclude that S is affinely equivalent to one of the sets $S_i(d)$, $i \in \{1, 2\}$ and $d \in \{1, 2, 4\}$, where

$$S_1(d) = \{0, u, d, d + 2u\} \text{ or } S_2(d) = \{0, 3u, d, d + 2u\}.$$

The lemma follows from the following claims:

- (i) $H(\mathbb{Z}_n, S_1(1)) \cong H(\mathbb{Z}_n, S_2(1))$.
- (ii) $H(\mathbb{Z}_n, S_1(1)) \cong_{\text{aff}} H(\mathbb{Z}_n, S_1(d))$ for $d \in \{2, 4\}$;
- (iii) $H(\mathbb{Z}_n, S_1(d)) \cong_{\text{aff}} H(\mathbb{Z}_n, S_2(d)) \iff d \in \{2, 4\} \text{ or } (d = 1 \text{ and } u \not\equiv 2 \pmod{4})$;

(i): Define the mapping $f : V \mapsto V$ by

$$f : x^\varepsilon \mapsto \begin{cases} x^\varepsilon & \text{if } x \in \{0, 1, \dots, u-1\} \cup \{2u, \dots, 3u-1\}, \\ (x + 2u)^\varepsilon & \text{otherwise.} \end{cases}$$

We leave for the reader to verify that f is in fact an isomorphism from $H(\mathbb{Z}_n, S_1(1))$ to $H(\mathbb{Z}_n, S_2(1))$ (compare the graphs in Figure 1; here the white vertices represent the color class \mathbb{Z}_n^+ , while the black ones represent the color class \mathbb{Z}_n^-).

(ii): Since $d \in \{2, 4\}$, u is an odd number. For $d \in \{2, 4\}$ define $r_d \in \mathbb{Z}_n^*$ as follows:

$$r_2 = \begin{cases} 2 + u & \text{if } u \equiv 1 \pmod{4}, \\ 2 + 3u & \text{if } u \equiv 3 \pmod{4}, \end{cases} \quad r_4 = \begin{cases} 4 + u & \text{if } u \equiv 3 \pmod{4}, \\ 4 + 3u & \text{if } u \equiv 1 \pmod{4}. \end{cases}$$

It can be directly checked that $r_d S_1(1) + u = S_1(d)$, so $H(\mathbb{Z}_n, S_1(1)) \cong_{\text{aff}} H(\mathbb{Z}_n, S_1(d))$ for $d \in \{2, 4\}$.

(iii): If u is odd, then $(2u + 1)S_1(d) = S_2(d)$, hence $H(\mathbb{Z}_n, S_1(d)) \cong_{\text{aff}} H(\mathbb{Z}_n, S_2(d))$. Since u is odd whenever $d \in \{2, 4\}$, we are left with the case that $d = 1$ and u is even. If also $u \equiv 0 \pmod{4}$, then $(u + 1)S_1(1) + 3u = S_2(1)$, and again $H(\mathbb{Z}_n, S_1(1)) \cong_{\text{aff}} H(\mathbb{Z}_n, S_2(1))$.

Suppose that $d = 1$ and $u \equiv 2 \pmod{4}$. We finish the proof by showing that in this case $H(\mathbb{Z}_n, S_1(1)) \not\cong_{\text{aff}} H(\mathbb{Z}_n, S_2(1))$. Suppose that, there is an affine transformation $\psi : x \mapsto$

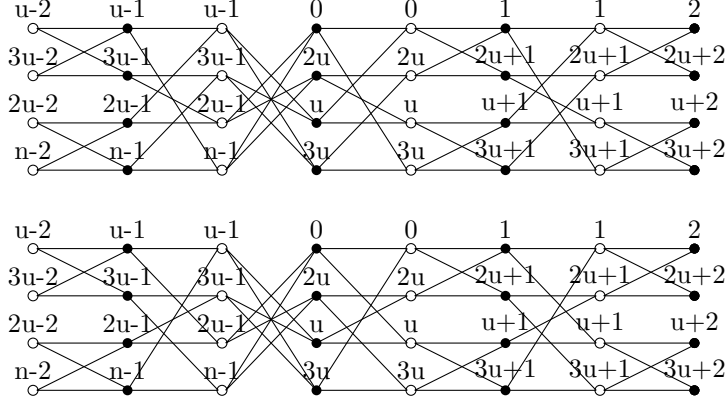


Figure 1: Haar graphs $H(\mathbb{Z}_n, S_1(1))$ and $H(\mathbb{Z}_n, S_2(1))$.

$rx + s$, $r \in \mathbb{Z}_n^*$ and $s \in \mathbb{Z}_n$, which maps the set $S_1(1)$ to $S_1(2)$. Then $1^\psi - (1 + 2u)^\psi = 2u$ in \mathbb{Z}_n . This implies that $\{1, 1 + 2u\}^\psi = \{1, 1 + 2u\}$ and $\{0, u\}^\psi = \{0, 3u\}$, and hence

$$r + s \in \{1, 1 + 2u\} \text{ and } r\{0, u\} + s = \{0, 3u\}.$$

A direct analysis shows that the above equations cannot hold if $u \equiv 2 \pmod{4}$. Thus $H(\mathbb{Z}_n, S_1(1)) \not\cong_{\text{aff}} H(\mathbb{Z}_n, S_2(1))$, this completes the proof of (iii). \blacksquare

Now, we turn to the case when $2u \neq m$. Recall that the canonical bicyclic group C is generated by the permutation c defined in (1). For a divisor $\ell \mid n$, C^ℓ will denote the subgroup of C generated by c^ℓ . It will be convenient to denote by δ_ℓ the partition of V into the orbits of C^ℓ , i.e., $\delta_\ell = \text{Orb}(C^\ell, V)$. Furthermore, we set $\eta_{n,\ell}$ for the homomorphism $\eta_{n,\ell} : \mathbb{Z}_n \rightarrow \mathbb{Z}_\ell$ defined by $\eta_{n,\ell}(1) = 1$.

Observe that, if δ_ℓ is, in addition, a system of blocks for the group $A = \text{Aut}(H(\mathbb{Z}_n, S))$, then an action of A can be defined on $H(\mathbb{Z}_\ell, \eta_{n,\ell}(S))$ by letting $g \in A$ act as

$$(x^\varepsilon)^g = y^\varepsilon \iff \{z^- : z \in \eta_{n,\ell}^{-1}(x)\}^g = \{z^- : z \in \eta_{n,\ell}^{-1}(y)\}, \quad x \in \mathbb{Z}_\ell, \quad \varepsilon \in \{+, -\}. \quad (4)$$

We denote the corresponding kernel by $A_{(\delta_\ell)}$, and the image of $g \in G$ by g^{δ_ℓ} . Note that, if X is a bicyclic group of $H(\mathbb{Z}_n, S)$, then $X^{\delta_\ell} = \{x^{\delta_\ell} : x \in X\}$ is a bicyclic group of $H(\mathbb{Z}_\ell, \eta_{n,\ell}(S))$.

Let $S = \{0, u, v, v + m\}$ be the subset of \mathbb{Z}_n defined in Theorem 3.1. Let δ be the partition of V defined by

$$\delta = \{X \cup X^{\psi_{1,0,0}} : X \in \text{Orb}(C^u, V)\}, \quad (5)$$

where $\psi_{1,0,0}$ is defined in (2). We write $\delta = \{V_0, \dots, V_{u-1}\}$, where

$$V_i = \{(iv + ju)^+, (iv + ju)^- : j \in \{0, 1, \dots, (n/u) - 1\}\}.$$

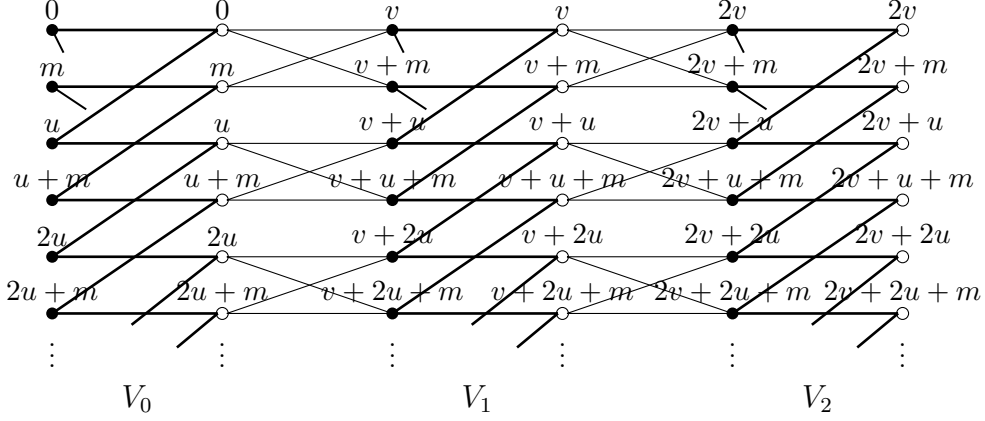


Figure 2: The Haar graph $H(\mathbb{Z}_n, S)$

A part of $H(\mathbb{Z}_n, S)$ is drawn in Figure 2 using the partition δ . White and black colors represent again the color classes \mathbb{Z}_n^+ and \mathbb{Z}_n^- , respectively. For $i \in \{0, 1, \dots, u-1\}$, let e_i be the involution of V defined by

$$e_i : x^\varepsilon \mapsto \begin{cases} (x+m)^\varepsilon & \text{if } x^\varepsilon \in V_i, \\ x^\varepsilon & \text{otherwise.} \end{cases}$$

It is clear that each $e_i \in \text{Aut}(H(\mathbb{Z}_n, S))$, and also that $e_i e_j = e_j e_i$ for all $i, j \in \{0, 1, \dots, u-1\}$. Let $E = \langle e_0, e_1, \dots, e_{u-1} \rangle$. Thus $E \leq \text{Aut}(H(\mathbb{Z}_n, S))$ and $E \cong \mathbb{Z}_2^u$. For a subset $I \subseteq \{0, 1, \dots, u-1\}$ let e_I be the element in E defined by $e_I = \prod_{i \in I} e_i$.

The following lemma about imprimitivity systems of blocks will be used throughout the paper.

Lemma 3.3. *Let $\Gamma = H(\mathbb{Z}_n, R)$ be a Haar graph and suppose that $T \subset R$ such that the point stabilizer $\text{Aut}(\Gamma)_{0+}$ fixes setwise T^- , and let $d = |\langle T - T \rangle|$, where $T - T = \{t_1 - t_2 : t_1, t_2 \in T\}$. The the partition π of V defined by*

$$\pi = \{X \cup X^{\psi_{1,t,-t}} : X \in \text{Orb}(C^{m/d}, V)\}, \text{ where } t \in T$$

*is a system of blocks for $\text{Aut}(\Gamma)$.*²

PROOF. Put $A = \text{Aut}(\Gamma)$. Since T is fixed setwise by A_{0+} , we may write

$$T = T_1 \cup \dots \cup T_k,$$

where T_i^- is an A_{0+} -orbit for every $i \in \{1, 2, \dots, k\}$. Choose an arc $(0^+, t_i^-)$ of Γ where we fix an element $t_i \in T_i$ for every $i \in \{1, \dots, k\}$. We claim that, the orbital graph of A containing $(0^+, t_i^-)$ is self-paired, and in fact it is equal to the Haar graph $H(\mathbb{Z}_n, T_i)$ (for a definition of an orbital graph, see [5]).

²Notice that, π does not depend of the choice of the element $t \in T$.

Define \bar{A} as the color preserving subgroup of A . Then $A = \bar{A} \rtimes \langle \psi_{-1,0,0} \rangle$. Also, $\bar{A} = A_{0^+}C$, as C is transitive on \mathbb{Z}_n^+ . Then the orbit of the arc $(0^+, t_i^-)$ under A is

$$\begin{aligned} (0^+, t_i^-)^A &= (0^+, t_i^-)^{A_{0^+}C\langle \psi_{-1,0,0} \rangle} = \{(0^+, t_i')^- : t_i' \in T_i\}^{C\langle \psi_{-1,0,0} \rangle} \\ &= \{(j^+, (j + t_i')^-) : t_i' \in T_i, j \in \mathbb{Z}_n\}^{\langle \psi_{-1,0,0} \rangle} \\ &= \{(j^+, (j + t_i')^-) : t_i' \in T_i, j \in \mathbb{Z}_n\} \cup \{((-j)^-, (-j - t_i')^+) : t_i' \in T_i, j \in \mathbb{Z}_n\}, \\ &= \{(j^+, (j + t_i')^-) : t_i' \in T_i, j \in \mathbb{Z}_n\} \cup \{((j + t_i')^-, j^+) : t_i' \in T_i, j \in \mathbb{Z}_n\}, \end{aligned}$$

which is clearly equal to the set of the set of arcs of $H(\mathbb{Z}_n, T_i)$. The claim is proved.

Since $H(\mathbb{Z}_n, T_i)$ is an orbital graph, $A \leq \text{Aut}(H(\mathbb{Z}_n, T_i))$. Combining this with $H(\mathbb{Z}_n, T) = \cup_{i=1}^k H(\mathbb{Z}_n, T_i)$, we have that $A \leq \text{Aut}(H(\mathbb{Z}_n, T))$. Let Σ be the connected component of $H(\mathbb{Z}_n, T)$ which contains 0^+ . Obviously, the set W of vertices contained in Σ is a block for A . It is easy to verify that $W = X \cup X^{\psi_{1,t,-t}}$ where X is the orbit of 0^+ under $C^{n/d}$. The lemma follows. \blacksquare

Lemma 3.4. *Let S be the set defined in Theorem 3.1. If $2u \neq m$, then the stabilizer $\text{Aut}(H(\mathbb{Z}_n, S))_{0^+}$ is given as follows.*

- (1) *If $u \not\equiv 2v \pmod{m/u}$, then $\text{Aut}(H(\mathbb{Z}_n, S))_{0^+} = E_{0^+}$.*
- (2) *If $u \equiv 2v \pmod{m/u}$, then $\text{Aut}(H(\mathbb{Z}_n, S))_{0^+} = E_{0^+} \times F$ for a subgroup $F \leq \text{Aut}(H(\mathbb{Z}_n, S))_{0^+}$, $|F| = 2$.*

PROOF. For short we put $\Gamma = H(\mathbb{Z}_n, S)$ and $A = \text{Aut}(\Gamma)$. Consider the partition δ defined in (5). Applying Lemma 3.3 with $R = S$, $T = \{0, u\}$ and $t = 0$, we obtain that δ is a system of blocks for A . The quotient graph Γ/δ is a u -circuit if $u > 2$ and a 2-path if $u = 2$. Let $g \in A_{0^+}$. Then g fixes the directed edge (V_0, V_1) of Γ/δ , hence it must fix all sets V_i . Thus $A_{0^+} \leq A_{(\delta)}$, where $A_{(\delta)}$ is the kernel of the action of A on δ .

Consider the action of A_{0^+} on V_0 . The corresponding kernel is $A_{(V_0)}$, the pointwise stabilizer of V_0 in A , and the corresponding image is a subgroup of $\text{Aut}(\Gamma[V_0])$, where $\Gamma[V_0]$ is the subgraph of Γ induced by V_0 . Using that $2u \neq m$, we show next that $A_{(V_0)} = E_{0^+}$. It is clear that $A_{(V_0)} \geq E_{0^+}$. We are going to prove that $A_{(V_0)} \leq E_{0^+}$ also holds. Let $g \in A_{(V_0)}$. Then for a suitable element $e \in \langle e_1 \rangle$ the product ge fixes pointwise V_0 and fix the vertex v^+ from block V_1 . Thus ge acts on V_1 as the identity or the unique reflection of the circuit $\Gamma[V_1]$ that fixes v^+ . If this action is not the identity, then ge switches v^- and $(v + n - u)^-$, and so it must switch $(v + u)^+$ and $(v + n - u)^+$. This implies that $(v + n - u)^+ = (v + u + m)^+$, contradicting that $2u \neq m$. We obtain that ge acts as the identity also on V_1 . Continuing in this way we find that ge' is the identity with a suitable choice of $e' \in E_{0^+}$, hence $g = e'$.

The equality $A_{(V_0)} = E_{0^+}$ together with $\text{Aut}(\Gamma[V_0]) \cong D_{4u}$ imply that $|A_{0^+} : E_{0^+}| \leq 2$. Moreover, $|A_{0^+} : E_{0^+}| = 2$ holds exactly when A_{0^+} contains an involution g for which $g : 0^- \leftrightarrow u^-$. In the latter case $A_{0^+} = E_{0^+} \times \langle g \rangle$ as g centralizes E (observe that g is in the kernel $A_{(\delta)}$, hence acts on a block V_i as an element of $D_{2n/u}$, while E acts on V_i as the center $Z(D_{2n/u})$.) We settle the lemma by proving the following equivalence :

$$A_{0^+} \cong E_{0^+} \times \mathbb{Z}_2 \iff u \equiv 2v \pmod{m/u}. \quad (6)$$

Suppose first that $A_{0^+} = E_{0^+} \times \langle g \rangle$, where $g \in A_{0^+}$ and $g : 0^- \leftrightarrow u^-$. By (c) of Theorem 3.1, $\{v^-, (v+m)^-\}^{A_{0^+}} = \{v^-, (v+m)^-\}$. Applying Lemma 3.3 with $R = S$, $T = \{v, v+m\}$ and $t = v$, we obtain that the set $B = \{0^+, m^+, v^-, (v+m)^-\}$ is a block for A . The induced graph $\Gamma[B]$ is a 4-circuit. Denote by $A_{\{B\}}$ the setwise stabilizer of B in A , and by $A_{\{B\}}^B$ the permutation group of B induced by $A_{\{B\}}$. As $\Gamma[B]$ is a 4-circuit, $A_{\{B\}}^B \leq D_8$. This gives that $\{0^+, m^+\}$ is a block for $A_{\{B\}}^B$, and therefore it is also a block for A . We conclude that $\delta_m = \{X : X \in \text{Orb}(C^m, V)\}$ is a system of blocks for A . Consider the action of A on $H(\mathbb{Z}_m, \eta_{n,m}(S))$ defined in (4). Then $E \leq A_{(\delta_m)}$, while $g \notin A_{(\delta_m)}$. This implies that g^{δ_m} is an automorphism of $H(\mathbb{Z}_m, \eta_{n,m}(S))$ which normalizes its canonical bicyclic group. This means that $g^{\delta_m} = \varphi_{r,s,t}$ for some $r \in \mathbb{Z}_m^*$ and $s, t \in \mathbb{Z}_m$. Using that $g^{\delta_m} : 0^+ \mapsto 0^+$ and $0^- \mapsto \eta_{n,m}(u)^-$, we find that $t = 0$ and $s = \eta_{n,m}(u)$, and so

$$A^{\delta_m} = \langle D^{\delta_m}, \varphi_{r, \eta_{n,m}(u), 0} \rangle. \quad (7)$$

Also, $g^{\delta_m} : \eta_{n,m}(u)^- \mapsto 0^-$ and $\eta_{n,m}(v)^- \mapsto \eta_{n,m}(v)^-$, hence $r\eta_{n,m}(u) = -\eta_{n,m}(u)$ and $r\eta_{n,m}(v) = \eta_{n,m}(v-u)$ hold in \mathbb{Z}_m . From these $r \equiv -1 \pmod{m/u}$ and $rv \equiv v-u \pmod{m/u}$, i.e., $u \equiv 2v \pmod{m/u}$. The implication “ \Rightarrow ” in (6) is now proved.

Suppose next that $u \equiv 2v \pmod{m/u}$. Define the permutation g of V by

$$g : (vi + uj)^\varepsilon \mapsto \begin{cases} (vi - (i+j)u)^+ & \text{if } \varepsilon = +, \\ (vi - (i+j-1)u)^- & \text{if } \varepsilon = -, \end{cases}$$

where $i \in \{0, 1, \dots, u-1\}$ and $j \in \{0, 1, \dots, n/u-1\}$. It can be verified directly that $g \in A_{0^+}$, $0^{+g} = 0^+$ and $g : 0^- \leftrightarrow u^-$, implying that $A_{0^+} = E_{0^+} \times \langle g \rangle$. Thus part “ \Leftarrow ” of (6) is also true. The lemma is proved. \blacksquare

Lemma 3.5. *Let S be the set defined in Theorem 3.1. If $2u \neq m$, then for the normalizer $N_{\text{Aut}(H(\mathbb{Z}_n, S))}(C)$ of C in $\text{Aut}(H(\mathbb{Z}_n, S))$,*

$$|\text{Aut}(H(\mathbb{Z}_n, S)) : N_{\text{Aut}(H(\mathbb{Z}_n, S))}(C)| = \begin{cases} 2^{u-2} & \text{if } 2 \mid u \text{ and } (u \not\equiv 2v \pmod{m/u} \text{ or } \\ & u/2 \equiv v \pmod{m/u}), \\ 2^{u-1} & \text{otherwise.} \end{cases} \quad (8)$$

PROOF. For short we put $A = \text{Aut}(H(\mathbb{Z}_n, S))$ and $N = N_A(C)$. Since $A = DA_{0^+}$ and $D \leq N$, $N = D(N \cap A_0^+)$. The cases (1) and (2) in Lemma 3.4 are considered separately.

CASE 1. $u \not\equiv 2v \pmod{m/u}$.

In this case, from Lemma 3.4, $A_{0^+} = E_{0^+}$, hence $|A| = 2^u n$. Let $g \in N \cap A_0^+$. Since $g \in E_{0^+}$, it follows quickly that $g = 1_A$ or $2 \mid u$ and $g = e_1 e_3 \cdots e_{u-1}$. Combining this with $N = D(N \cap G_0^+)$ we find that $|N| = 4n$ if $2 \mid u$, and $|N| = 2n$ if $2 \nmid u$. Formula (8) follows.

CASE 2. $u \equiv 2v \pmod{m/u}$.

From Lemma 3.4, $A_{0+} = E_{0+} \times F$ for a subgroup $F \leq A_{0+}$, $|F| = 2$, hence $|A| = 2^{u+1}n$. It follows from the proof of Lemma 3.4 that, there exists $r \in \mathbb{Z}_m^*$ such that the following hold:

$$r\eta_{n,m}(u) = -\eta_{n,m}(u) \text{ and } r\eta_{n,m}(v) = \eta_{n,m}(v - u).$$

Let $s \in \mathbb{Z}_n^*$ such that $\eta_{n,m}(s) = r$. Then

$$su \in \{-u, -u + m\} \text{ and } sv \in \{v - u, v - u + m\}. \quad (9)$$

Suppose that $2 \nmid u$. Then we get as before that $N \cap E_{0+}$ is trivial. Notice also that, $u \equiv 2v + m/u \pmod{n/u}$, which follows from the assumption that $u \equiv 2v \pmod{m/u}$ and that $2 \nmid u$. Thus $2 \nmid m$ and $2 \mid (u + m)$, implying that in (9) we have $su = -u$. We obtain that $\varphi_{s,u,0} \in N \cap (A_{0+} \setminus E_{0+})$, and so $|N \cap A_{0+}| = 2$.

Suppose next that $2 \mid u$. Then $|N \cap E_{0+}| = 2$. It is easily seen that $|N \cap A_{0+}| = 4$ if and only if there exists $r \in \mathbb{Z}_n^*$ such that $ru = -u$ and $rv = v - u$ hold in \mathbb{Z}_n . Consider the following system of linear congruences:

$$xu \equiv u \pmod{n}, \quad xv \equiv v - u \pmod{n}. \quad (10)$$

From the first congruence we can write x in the form $x = yn/u - 1$. Substitute this into the second congruence. We obtain that $yvn/u \equiv 2v - u \pmod{n}$. This has a solution if and only if $\gcd(vn/u, n) \mid (2v - u)$. Suppose that $\gcd(v, n) \neq 1$. Using that $\langle u, v \rangle = \mathbb{Z}_n$ and that $2 \mid u$, we obtain that $\gcd(v, m/u) \neq 1$. However, then from the assumption that $u \equiv 2v \pmod{m/u}$ it follows that also $\gcd(v, u) \neq 1$, which contradicts that $\langle u, v \rangle = \mathbb{Z}_n$. Hence $\gcd(v, n) = 1$, $\gcd(vn/u, n) = n/u$, and so (10) has a solution if and only if $u \equiv 2v \pmod{n/u}$, or equivalently, $u/2 \equiv v \pmod{m/u}$ (recall that $2 \mid u$ and $u \mid m$). It is not hard to show that any solution to (10) is necessarily prime to n , hence is in \mathbb{Z}_n^* . The above arguments can be summarized as follows: $|N| = 8n$ if $2 \mid u$ and $u/2 \equiv v \pmod{m/u}$, and $|N| = 4n$ otherwise. This is consistent with (8). The lemma is proved. ■

Lemma 3.6. *Let $r \in \mathbb{Z}_n^*$, $r \neq 1$ and $s \in \mathbb{Z}_n$ such that the permutation $\varphi_{r,s,0}$ is of order 2. Then the group $\langle D, \varphi_{r,s,0} \rangle$ contains a bicyclic subgroup different from C if and only if $8 \mid n$, $r = n/2 + 1$, and $s = 0$ or $s = n/2$.*

PROOF. Suppose that $\langle D, \varphi_{r,s,0} \rangle$ contains a bicyclic subgroup X such that $X \neq C$. Then X is generated by a permutation in the form $c^i \varphi_{r,s,0}$. Since $\varphi_s^2 = id_V$, $r^2 = 1$ in \mathbb{Z}_n , and we calculate that $(c^i \varphi_{r,s,0})^2$ sends x^+ to $(x + r(r+1)i)^+$ for every $x \in \mathbb{Z}_n$. That \mathbb{Z}_n^+ is an orbit of X is equivalent to the condition that $\gcd(n, r+1) = 2$. Using this and that $r^2 - 1 = (r-1)(r+1) \equiv 0 \pmod{n}$, we find that $n/2$ divides $r-1$, so $r = 1$ or $r = n/2 + 1$. Since $r \neq 1$, we have that $r = n/2 + 1$ and $8 \mid n$. Then $(\varphi_{r,s,0})^2$ sends x^- to $(x + (n/2 + 2)s)^-$. Since $(\varphi_{r,s,0})^2 = id_V$, we obtain that $s = 0$ or $s = n/2$.

On the other hand, it can be directly checked that, if $8 \mid n$, $r = n/2 + 1$ and $s \in \{0, n/2\}$, then the permutation $c\varphi_{r,s,0}$ generates a bicyclic subgroup of $\langle D, \varphi_{r,s,0} \rangle$. Obviously, this bicyclic subgroup cannot be C . The lemma is proved. ■

Everything is prepared to prove the main result of the section.

PROOF OF THEOREM 3.1. The case that $2u = m$ is settled already in Lemma 3.2, hence let $2u \neq m$. We consider the action of $A = \text{Aut}(H(\mathbb{Z}_n, S))$ on the system of blocks δ_m defined in (4). We claim that the corresponding image A^{δ_m} has a unique bicyclic subgroup (which is, of course, C^{δ_m}).

This is easy to see if $A_{0+} = E_{0+}$, because in this case $A^{\delta_m} = (DA_{0+})^{\delta_m} = D^{\delta_m}$.

Let $A_{0+} \neq E_{0+}$. Then $A_{0+} = E_{0+} \times F$ for some subgroup F , $|F| = 2$. By (7), $A^{\delta_m} = \langle D^{\delta_m}, \varphi_{r, \eta_{n,m}(u), 0} \rangle$. Also, $r \equiv -1 \pmod{m/u}$, hence $r \neq 1$ in \mathbb{Z}_m . By Lemma 3.5, A^{δ_m} contains more than one bicyclic subgroup if and only if $8 \mid m$, $r = m/2 + 1$ and $\eta_{n,m}(u) \in \{0, m/2\}$. In the latter case $u \in \{m, m/2\}$, which is impossible as $u < m/2$. Hence A^{δ_m} contains indeed a unique bicyclic subgroup.

We calculate below the number of bicyclic groups of $H(\mathbb{Z}_n, S)$; we denote this number by \mathbb{B} . Since $G = DA_{0+}$, every $g \in G$ can be written as $g = xy$ with $x \in D$ and $y \in A_{0+}$. If $\langle g \rangle$ is a bicyclic group of $H(\mathbb{Z}_n, S)$, then $\langle g \rangle^{\delta_m}$ is a bicyclic subgroup of A^{δ_m} , and so $\langle g \rangle^{\delta_m} = C^{\delta_m}$. This implies that $x = c^i \in C$ for some $i \in \{1, \dots, n-1\}$ with $\gcd(i, m) = 1$, and that $y \in E_{0+}$. Then $y = e_I$ for a subset $I \subseteq \{1, \dots, u-1\}$. It follows by induction that

$$(c^i e_I)^u = c^{ui} e_{I+u} \cdots e_{I+(u-1)u}.$$

Here for $k \in \{1, \dots, u-1\}$, the set $I + ki = \{x + ki : x \in I\}$, where addition is taken modulo u . Since $\gcd(i, m) = 1$ and $u \mid m$, $\gcd(i, u) = 1$, from which

$$e_I e_{I+u} \cdots e_{I+(u-1)u} = (e_0 e_1 \cdots e_{u-1})^{|I|} = c^{m|I|}.$$

Therefore, $(c^i e_I)^u = c^{u(i + \frac{m}{u}|I|)}$. This shows that $\langle c^i e_I \rangle$ is a bicyclic group if and only if $c^i e_I$ is of order n , or equivalently,

$$\gcd\left(i + \frac{m}{u}|I|, \frac{2m}{u}\right) = 1. \quad (11)$$

Let $2 \mid (m/u)$. Then $2 \mid m$ and i is odd. Hence (11) always holds. We obtain that the number of elements in A which generate a bicyclic group is $\phi(n)2^{u-1}$, where ϕ denotes the Euler's totient function. This implies that $\mathbb{B} = 2^{u-1}$.

Suppose next that $2 \nmid (m/u)$. Now, if $2 \mid u$, then $2 \mid m$, hence $2 \nmid i$, and so (11) is true if and only if $|I|$ is even. We deduce from this that $\mathbb{B} = 2^{u-2}$.

Finally, if $2 \nmid u$, then $2 \nmid m$, and in this case (11) holds if and only if $\gcd(i, n) = 1$ and $|I|$ is even, or $\gcd(i, n) = 2$ and $|I|$ is odd. We calculate that $\mathbb{B} = 2^{u-1}$. All cases have been considered, our calculations are summarized in the formula:

$$\mathbb{B} = \begin{cases} 2^{u-2} & \text{if } 2 \mid u \text{ and } 2 \nmid (m/u), \\ 2^{u-1} & \text{otherwise.} \end{cases} \quad (12)$$

Let Ξ be a bicyclic base of $H(\mathbb{Z}_n, S)$. By (8) and (12) we obtain that, $|\Xi| > 1$ if and only if

$$|A : N_A(C)| = 2^{u-2} \text{ and } \mathbb{B} = 2^{u-1}.$$

This happens exactly when

$$(2 \mid u \text{ and } (u \not\equiv 2v \pmod{m/u} \text{ or } u/2 \equiv v \pmod{m/u})) \text{ and } (2 \nmid u \text{ or } 2u \mid m).$$

After some simplification,

$$|\Xi| > 1 \iff 2 \mid u, 2u \mid m \text{ and } u/2 \not\equiv v + m/(2u) \pmod{m/u}.$$

Suppose that $|\Xi| > 1$. Then A contains exactly 2^{n-1} bicyclic subgroups, 2^{n-2} of which are conjugate to C . These 2^{n-1} subgroups are enumerated as: $\langle ce_I \rangle$, $I \subseteq \{1, \dots, u-1\}$. For $i \in \{1, \dots, u-2\}$, $e_i ce_i = ce_{\{i, i+1\}}$. We can conclude that the bicyclic subgroups split into two conjugacy classes:

$$\{\langle ce_I \rangle : I \subseteq \{1, \dots, u-1\}, |I| \text{ is even} \} \text{ and } \{\langle ce_I \rangle : I \subseteq \{1, \dots, u-1\}, |I| \text{ is odd} \}.$$

In particular, $|\Xi| = 2$. Choose ξ from $\text{Sym}(V)$ which satisfies

$$\xi c \xi^{-1} = ce_1 \text{ and } \xi : 0^+ \mapsto 0^+, 0^- \mapsto 0^-.$$

Then Ξ can be chosen as $\Xi = \{id_V, \xi\}$. Also, $\{v^-, (v+m)^-\}^\xi = \{v^-, (v+m)^-\}$, and since $(ce_1)^{u+m} = c^u$, $(u^-)^\xi = (0^-)^{(ce_1)^{u+m}\xi} = (0^-)^{\xi c^{u+m}} = (u+m)^-$. Thus $H(\mathbb{Z}_n, S)^\xi = H(\mathbb{Z}_n, \{0, u+m, v, v+m\})$. The theorem follows from Theorem 2.5. \blacksquare

4 Proof of Theorem 1.1

Theorem 1.1 follows from Theorem 3.1 and the following theorem.

Theorem 4.1. *Let $H(\mathbb{Z}_n, S)$ be a connected Haar graph such that $|S| = 4$ and S is not a BCI-subset. Then $n = 2m$, and there exist $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n$ such that $aS + b = \{0, u, v, v+m\}$ and the conditions (a)-(c) in Theorem 3.1 hold.*

Before we prove Theorem 4.1 it is necessary to give three preparatory lemmas. For an element $i \in \mathbb{Z}_n$, we denote by $|i|$ the order of i viewed as an element of the additive group \mathbb{Z}_n . Thus we have $|i| = n/\gcd(n, i)$.

Lemma 4.2. *If $R = \{i, n-i, j\}$ is a generating subset of \mathbb{Z}_n with $|i|$ odd, then R is a CI-subset.*

PROOF. For short we put $A = \text{Aut}(\text{Cay}(\mathbb{Z}_n, R))$ and denote by A_0 the stabilizer of $0 \in \mathbb{Z}_n$ in A . Clearly, A_0 leaves R fixed. If A_0 acts on R trivially, then $A \cong \mathbb{Z}_n$, and the lemma follows by Theorem 2.1. If A_0 acts on R transitively, then $\text{Cay}(\mathbb{Z}_n, R)$ is edge-transitive. This condition forces that R is a CI-subset (see [10, page 320]).

We are left with the case that R consists of two orbits under A_0 . These orbits must be $\{i, n-i\}$ and $\{j\}$. It is clear that A_0 leaves the subgroups $\langle i \rangle$ and $\langle j \rangle$ fixed; moreover, the latter set is fixed pointwise, and since $|i|$ is odd, $\langle i \rangle$ consists of $(|i|-1)/2$ orbits under A_0 , each of length 2, and one orbit of length 1. We conclude that $\mathbb{Z}_n = \langle i \rangle \times \langle j \rangle$, and also that A

is permutation isomorphic to the permutation direct product $((\mathbb{Z}_{|i|})_{\text{right}} \rtimes \langle \pi \rangle) \times (\mathbb{Z}_{|j|})_{\text{right}}$. For $\ell \in \{|i|, |j|\}$, $(\mathbb{Z}_\ell)_{\text{right}}$ is generated by the affine transformation $x \mapsto x + 1$, and π is the affine transformation $x \mapsto -x$. We leave for the reader to verify that the above group has a unique regular cyclic subgroup. The lemma follows by Theorem 2.1. \blacksquare

Lemma 4.3. *Let $n = 2m$ and $R = \{i, n - i, j, j + m\}$ be a subset of \mathbb{Z}_n such that*

(a) *R generates \mathbb{Z}_n ;*

(b) *$|i|$ is odd;*

(c) *the stabilizer $\text{Aut}(\text{Cay}(\mathbb{Z}_n, R))_0$ leaves the set $\{i, n - i\}$ setwise fixed.*

Then R is a CI-subset.

PROOF. For short we put $A = \text{Aut}(\text{Cay}(\mathbb{Z}_n, R))$. Let T be a subset of \mathbb{Z}_n such that $\text{Cay}(\mathbb{Z}_n, R) \cong \text{Cay}(\mathbb{Z}_n, T)$ and let f be an isomorphism from $\text{Cay}(\mathbb{Z}_n, R)$ to $\text{Cay}(\mathbb{Z}_n, T)$ such that $f(0) = 0$.

Let us consider the subgraphs $\Gamma_1 := \text{Cay}(\mathbb{Z}_n, \{i, n - i\})$ and $\Gamma_2 := \text{Cay}(\mathbb{Z}_n, \{j, j + m\})$. By condition (c), the group A preserves both of these subgraphs, that is, $A \leq \text{Aut}(\Gamma_i)$ for $i \in \{1, 2\}$. Therefore, $f^{-1}(\mathbb{Z}_n)_{\text{right}} f \leq A \leq \text{Aut}(\Gamma_i)$, implying that f maps Γ_i to a Cayley graph $\text{Cay}(\mathbb{Z}_n, T_i)$ for both $i \in \{1, 2\}$. Clearly, $T = T_1 \cup T_2$. Since $\Gamma_1 = \text{Cay}(\mathbb{Z}_n, \{i, n - i\}) \cong \text{Cay}(\mathbb{Z}_n, T_1)$ it follows by a result of Sun [15] (see also [10]), that $T_1 = a\{i, n - i\}$ for some $a \in \mathbb{Z}_n^*$. Letting $t_1 = ai$, we have $T_1 = \{t_1, n - t_1\}$ such that $|i| = |t_1|$. In the same way $T_2 = a'\{j, j + m\}$ for some $a' \in \mathbb{Z}_n^*$, and letting $t_2 = a'j$, we have $T_2 = \{t_2, t_2 + m\}$ such that $|t_2| = |j|$. Since $f(0) = 0$, f maps $\{i, n - i\}$ to $T_1 = \{t_1, n - t_1\}$ and $\{j, j + m\}$ to $T_2 = \{t_2, t_2 + m\}$.

We claim that the partition of \mathbb{Z}_n into the cosets of $\langle m \rangle$ is a system of blocks for $\text{Aut}(\Gamma_1)$, hence also for the group $A \leq \text{Aut}(\Gamma_1)$. Let us put $\bar{A} = \text{Aut}(\Gamma_1)$. It easily seen that \bar{A}_0 is transitive on $\{j, j + m\}$. Therefore, by considering the action of \bar{A}_0 on the set $\{j, j + m\}$ we find that $\bar{A}_0 = \bar{A}_{0,j} \langle m_{\text{right}} \rangle = \langle m_{\text{right}} \rangle \bar{A}_{0,j}$, where $\bar{A}_{0,j} = \bar{A}_0 \cap \bar{A}_j$, and m_{right} is the permutation $x \mapsto x + m$ for every $x \in \mathbb{Z}_n$. From this $\bar{A}_0 \langle m_{\text{right}} \rangle = \langle m_{\text{right}} \rangle \bar{A}_0$. This means $\bar{A}_0 \langle m_{\text{right}} \rangle$ is a subgroup of \bar{A} which clearly contains \bar{A}_0 . It is well-known that the orbit $\text{Orb}_{\bar{A}_0 \langle m_{\text{right}} \rangle}(0)$ is a block for \bar{A} . Now the required statement follows as $\text{Orb}_{\bar{A}_0 \langle m_{\text{right}} \rangle}(0) = 0^{\bar{A}_0 \langle m_{\text{right}} \rangle} = 0^{\langle m_{\text{right}} \rangle} = \langle m \rangle$.

Since the partition of \mathbb{Z}_n into the cosets of $\langle m \rangle$ is a system of blocks for A , the isomorphism f induces an isomorphism from $\text{Cay}(\mathbb{Z}_m, \eta_{n,m}(R))$ to $\text{Cay}(\mathbb{Z}_m, \eta_{n,m}(T))$, we denote this isomorphism by \bar{f} . Note that, $\bar{f}(0) = 0$ for the identity element $0 \in \mathbb{Z}_m$.

The set $\eta_{n,m}(R)$ satisfies the conditions (a)-(c) of Lemma 4.2, hence it is a CI-subset. This means that \bar{f} is equal to a permutation $x \mapsto rx$ for some $r \in \mathbb{Z}_m^*$. Let $s \in \mathbb{Z}_n^*$ such that $\eta_{n,m}(s) = r$. Then $\eta_{n,m}(si) = \eta_{n,m}(s)\eta_{n,m}(i) = \eta_{n,m}(t_1)$, and so the following holds in \mathbb{Z}_n :

$$si = t_1 \text{ or } si = t_1 + m. \quad (13)$$

The order $|t_1| = |i|$ is odd by (b), implying that $|t_1| \neq |t_1 + m|$, and so $si = t_1$ holds in (13). We conclude that $sR = T$, so R is a CI-subset. The lemma is proved. \blacksquare

Lemma 4.4. *Let $n = 2m$ and $S = \{0, u, v, v + m\}$ such that*

- (a) *S generates \mathbb{Z}_n ;*
- (b) *$1 < u < n$, $u \mid n$ but $u \nmid m$;*
- (c) *$\text{Aut}(H(\mathbb{Z}_n, S))_{0^+}$ leaves the set $\{0^-, u^-\}$ setwise fixed.*

Then S is a BCI-subset.

PROOF. Let δ be the partition of V defined in (5). Applying Lemma 3.3 with $R = S$, $T = \{0, u\}$ and $t = 0$, we obtain that δ is a system of blocks for $A = \text{Aut}(H(\mathbb{Z}_n, S))$. Thus the stabilizer A_{0^+} leaves the set V_0 setwise fixed, and we may consider the action of A_{0^+} on V_0 . The subgraph of $H(\mathbb{Z}_n, S)$ induced by the set V_0 is a circuit of length $2n/u$, thus A_{0^+} fixes also the vertex on this circuit antipodal to 0^+ . We find that this antipodal vertex is $(u/2 + m)^-$. Therefore, $A_{0^+} = A_{(m+u/2)^-}$, and thus S is a BCI-subset if and only if $S - u/2 + m$ is a CI-subset of \mathbb{Z}_n , see Proposition 2.7. The latter set is

$$S - u/2 + m = \{u/2 + m, -u/2 + m, v - u/2, v - u/2 + m\}.$$

Since $u \nmid m$, u is even and the order $|u/2 + m|$ is odd. Lemma 4.3 is applicable to the set $S - u/2 + m$ (choose $i = u/2 + m$ and $j = v - u/2$), it gives us that $S - u/2 + m$ is a CI-subset. This completes the proof. \blacksquare

PROOF OF THEOREM 4.1. Let S be the subset of \mathbb{Z}_n given in Theorem 4.1. We deal first with the case when the canonical bicyclic group C is normal in $A = \text{Aut}(H(\mathbb{Z}_n, S))$.

CASE 1. $C \trianglelefteq A$.

By Theorem 2.5 there is a bicyclic group X of $H(\mathbb{Z}_n, S)$ such that $X \neq C$. Since $C \trianglelefteq A$, X is generated by a permutation in the form $c^i \varphi_{r,s,0}$, $r \in \mathbb{Z}_n^*$, $s \in \mathbb{Z}_n$, and $\text{ord}(\varphi_{r,s,0}) \geq 2$. The permutation $\varphi_{r,s,0}$ acts on both \mathbb{Z}_n^+ and \mathbb{Z}_n^- as an affine transformation. This fact together with the connectedness of $H(\mathbb{Z}_n, S)$ imply that, $\varphi_{r,s,0}$ acts faithfully on S^- . Thus $\text{ord}(\varphi_{r,s,0}) \leq 4$.

Suppose that $\text{ord}(\varphi_{r,s,0}) = 4$. We may assume without loss of generality that S^- can be obtained as $S^- = \{(0^-)^{\varphi_{r,s,0}^j} : j \in \{0, 1, 2, 3\}\}$, and so $S = \{0, s, (r+1)s, (r^2+r+1)s\}$ and $(r^3+r^2+r+1)s = 0$. Since $H(\mathbb{Z}_n, S)$ is connected, $\gcd(s, n) = 1$, and $(r+1)(r^2+1) = 0$. We find that $(c^i \varphi_{r,s,0})^4$ sends x^+ to $(x + r(r+1)(r^2+1)i)^+ = x^+$. Since $X = \langle c^i \varphi_{r,s,0} \rangle$ is bicyclic, $n = 4$, and so $H(\mathbb{Z}_n, S) \cong K_{4,4}$. This, however, contradicts that $C \trianglelefteq A$.

Now, suppose that $\text{ord}(\varphi_{r,s,0}) = 3$. If A_{0^+} is transitive on S^- , then it must be regular [9, Theorem 4.3]. This implies that S^- splits into two orbits under A_{0^+} with length 1 and 3, respectively. Let $s \in S$ such that $\{s^-\}$ is an orbit under A_{0^+} . Then $A_{0^+} = A_{s^-}$, and by Proposition 2.7, $S - s$ is not a CI-subset of \mathbb{Z}_n . However, in this case the graph $\text{Cay}(\mathbb{Z}_n, S - s)$ is edge-transitive, and thus $S - a$ is a CI-subset (see [10, page 320]), which is a contradiction.

Finally, suppose that $\text{ord}(\varphi_{r,s,0}) = 2$. If $r = 1$, then $2 \mid n$ and $s = m$, where $n = 2m$. This implies that S^- is a union of two orbits of C^m , we may write $S = \{0, m, s, s + m\}$.

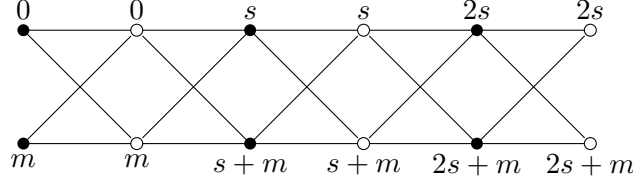


Figure 3: The lexicographical product $C_n[K_2^c]$.

The graph $H(\mathbb{Z}_n, S)$ is then isomorphic to the lexicographical product $C_n[K_2^c]$ of an n -circuit C_n with the graph K_2^c , see Figure 3. It is easily seen that then A_{0+} is not faithful on the set S^- , which is a contradiction.

Let $r \neq 1$. By Lemma 3.6, $8 \mid n$, $r = m + 1$ and $s \in \{0, m\}$, where $n = 2m$. We consider here only the case when $s = 0$ (the case when $s = m$ can be treated in the same manner). Then \mathbb{Z}_n^- splits into the following orbits under $\varphi_{r,s,0}$:

$$\{i^-\}, \{(i+1)^-, (i+1+m)^-\}, \text{ where } i \in \{0, 2, \dots, n-2\}.$$

Since $H(\mathbb{Z}_n, S)$ is connected, S^- contains one orbit of length 2 and two orbits of length 1. Let S_1 denote the orbit of length 2 and let $S_2 = S \setminus S_1$. The elements of S_2 are even. Let $S_2 = \{s, s'\}$ and let $u = \gcd(s - s', n)$. Then u is a divisor of n and also $2 \mid u$. There exist $a \in \mathbb{Z}_n^*$ such that $a(s - s') \equiv u \pmod{n}$. Now, choosing $b = -as'$ (all arithmetic is done in \mathbb{Z}_n), we find that $aS_2 + b = \{0, u\}$. It is clear that $aS_1 + b = \{v, v + m\}$ for some $v \in \mathbb{Z}_n$. We finish the proof of this case by showing that the set $R = \{0, u, v, v + m\}$ satisfies the conditions (a)-(c) of Theorem 3.1.

(a): As $H(\mathbb{Z}_n, S)$ is connected, $H(\mathbb{Z}_n, R)$ is also connected. This implies that u, v generate \mathbb{Z}_n .

(c): Since $C \trianglelefteq A$, $C \trianglelefteq \text{Aut}(H(\mathbb{Z}_n, R))$. To the contrary assume that $\text{Aut}(H(\mathbb{Z}_n, R))_{0+}$ does not leave $\{0^-, u^-\}$ fixed. Thus there exists some $g \in A_{0+}$ which maps v^- into $\{0^-, u^-\}$. Letting $w_1^- = (v^-)^g$ and $w_2^- = ((v+m)^-)^g$, we find that $w_1 - w_2 = m$, and from this that $u = m$. However, then $H(\mathbb{Z}_n, R) \cong C_n[K_2^c]$, which we have already excluded above. Thus $\text{Aut}(H(\mathbb{Z}_n, R))_{0+}$ fixes setwise $\{0^-, u^-\}$.

(b): We have already showed (see previous paragraph) that $u \neq m$ and $1 < u$. Since S is not a BCI-subset, R is also not a BCI-subset. This also implies that $u \mid m$ by Lemma 4.4, and we conclude that $1 < u < m$ and $u \mid m$, as required.

CASE 2. $C \not\trianglelefteq A$.

Let A_{0+} act transitively on S^- . This gives that $H(\mathbb{Z}_n, S)$ is edge-transitive. Since $C \not\trianglelefteq A$, $D \not\trianglelefteq A$, in other words, $H(\mathbb{Z}_n, S)$ is non-normal as a Cayley graph over the dihedral group D . We apply [8, Theorem 1.2], and obtain that $H(\mathbb{Z}_n, S)$ is either isomorphic to $K_n[K_2^c]$, or to one of 5 graphs of orders 10, 14, 26, 28 and 30, respectively. A direct check by computer shows that none of these graphs is possible as all corresponding subsets are BCI-subsets.

The set S^- cannot split into two orbits under A_{0+} of size 1 and 3, respectively (see the argument above). We are left with the case that $S = S_1 \cup S_2$, $|S_1| = |S_2|$, and A_{0+} leaves both sets S_1 and S_2 fixed. For $i \in \{1, 2\}$, let $n_i = |\langle S_i - S_i \rangle|$, $n_1 \leq n_2$, where $S_i - S_i = \{a - b : a, b \in S_i\}$.

We claim that $n_1 = 2$. To the contrary assume that $n_1 > 2$. We prove first that $C^{n/n_1} \trianglelefteq A$. Applying Lemma 3.3 with $R = S$, $T = S_1$ and $t = s_1 \in S_1$, we obtain that the partition

$$\delta = \{X \cup X^{\psi_{1,s_1,-s_1}} : X \in \text{Orb}(C^{n/n_1}, V)\},$$

is a system of blocks for A . Let us consider the action of $A_{(\delta)}$ (the kernel of A acting on δ) on the block of δ which contains 0^+ . Denote this block by Δ , and by Δ' the block which contains s^- for some $s \in S_2$. Notice that, the subgraph of $H(\mathbb{Z}_n, S)$ induced by any block of δ is a circuit of length $2n_1$, and when deleting these circuits, the rest splits into pairwise disjoint circuits of length $2n_2$. Let Σ denote the unique $(2n_2)$ -circuit through s^- . Now, suppose that $g \in A_{(\delta)}$ which fixes Δ pointwise. If $V(\Sigma) \cap \Delta = \{0^+\}$, then g must fix the edge $\{0^+, s^-\}$, and so fixes also s^- . If $V(\Sigma) \cap \Delta \neq \{0^+\}$, then $|V(\Sigma) \cap \Delta| = n_2 > 2$. This implies that g fixes every vertex on Σ , in particular, also s^- . The block Δ' has at least n_1 vertices having a neighbor in Δ , hence by the previous argument we find that all are fixed by g . Since $n_1 > 2$, Δ' is fixed pointwise by g . It follows, using the connectedness of $H(\mathbb{Z}_n, S)$, that $g = id_V$, hence that $A_{(\delta)}$ is faithful on Δ . Thus C^{n/n_1} is a characteristic subgroup of $A_{(\delta)}$, and since $A_{(\delta)} \trianglelefteq A$, $C^{n/n_1} \trianglelefteq A$.

Let G be the unique normal subgroup of A that fixes the color classes \mathbb{Z}_n^+ and \mathbb{Z}_n^- . We consider $N = G \cap C_A(C^{n/n_1})$. Then $C \leq N$ and $N \trianglelefteq A$. Pick $g \in N_{0+}$ such that g acts non-trivially on S^- . Since N centralizes C^{n/n_1} , g fixes pointwise the orbit of 0^+ under C^{n/n_1} , and hence also Δ . Then g^2 fixes S^- pointwise, and so also Δ' . We conclude that $g^2 = id_V$, and that either $N = C$, or $N = C \rtimes \langle g \rangle$. The case $N = C$ is impossible because $C \not\trianglelefteq A$. Let $N = C \rtimes \langle g \rangle$. Then $(S_i^-)^g = S_i^-$ (for both $i \in \{1, 2\}$), hence S_i is a union of orbits of g . As g normalizes C , $g = \varphi_{r,s,1}$. Recall that $\text{ord}(g) = 2$. If $r \neq 1$, then by Lemma 3.6, either C is the unique cyclic subgroup of N , or $8 \mid n$, $r = n/2 + 1$ and $s = 0$ or $s = n/2$. In the former case C is characteristic in N , and since $N \trianglelefteq A$, $C \trianglelefteq A$, a contradiction. Therefore, we are left with the case that $r = 1$ (and so $s = n/2$), or $8 \mid n$, $r = n/2 + 1$ and $s = 0$ or $s = n/2$. Then every orbit of g of length 2 and contained in \mathbb{Z}_n^- is in the form $\{j^-, (j+m)^-\}$ as we proved in Case 1. Since $n_i > 2$, we see that S_i^- must be fixed pointwise by g for both $i \in \{1, 2\}$. Thus S^- is fixed pointwise by g , implying that $g = id_V$. This is a contradiction, and so $n_1 = 2$.

Then $2 \mid n$ and we can write $S_1 = \{s, s+m\}$, where $n = 2m$. There exist $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n$ such that $aS_2 + b = \{0, u\}$ for some divisor u of n . Clearly, $aS_1 + b = \{v, v+m\}$ with $v = as + b$. We finish the proof of this case by showing that the set $R = \{0, u, v, v+m\}$ satisfies the conditions (a)-(c) of Theorem 3.1.

(a): As $H(\mathbb{Z}_n, S)$ is connected, $H(\mathbb{Z}_n, R)$ is also connected. This implies that u, v generate \mathbb{Z}_n .

(c): Since S_1 and S_2 are left fixed by A , $\text{Aut}(H(\mathbb{Z}_n, R))_{0+}$ leaves the set $\{0^-, u^-\}$ fixed.

(b): If $u = 1$, then $\text{Aut}(H(\mathbb{Z}_n, \{0, u\})) \leq D_{4n}$. But then $C \trianglelefteq A$, which is a contradiction. We conclude that $1 < u$, and by Lemma 4.4 that $u \mid m$ also holds, i.e., $1 < u < m$ and $u \mid m$, as required. ■

References

- [1] L. Babai, Isomorphism problem for a class of point-symmetric structures, *Acta Math. Acad. Sci. Hungar.* **29** (1977), 329–336.
- [2] M. Boben, T. Pisanski, A. Žitnik, I-graphs and the corresponding configurations, *J. Combin. Designs* **13** (2005), 406–424.
- [3] T. G. Boreham, I.Z. Bouwer and R. W. Frucht, A useful family of bicubic graphs, *Graphs Combin.* (1973), 213–225.
- [4] W. Bosma, J. Cannon, and C. Playoust, The MAGMA Algebra System I: The User Language, *J. Symbolic Comput.* **24** (1997), 235–265.
- [5] J. D. Dixon and B. Mortimer, Permutation groups, Graduate Texts in Mathematics 163, Springer-Verlag 1996.
- [6] M. Hladnik, D. Marušič, and T. Pisanski, Cyclic Haar graphs, *Discrete Math.* **244** (2002), 137–152.
- [7] W. Jin, W. Liu, A classification of nonabelian simple 3-BCI-groups, *European J. Combin.* **31** (2010), 1257–1264.
- [8] I. Kovács, B. Kuzman and A. Malnič, On non-normal arc transitive 4-valent dihedrants, *Acta Math. Sinica (Engl. ser.)* (8) **26** (2010), 1485–1498.
- [9] I. Kovács, B. Kuzman, A. Malnič and S. Wilson, Characterization of edge-transitive 4-valent bicirculants, *J. Graph Theory.* **69** (2012), 441–463.
- [10] C. H. Li, On isomorphisms of finite Cayley graphs - a survey, *Discrete Math.* **256** (2002), 301–334.
- [11] M. Muzychuk, On the isomorphism problem for cyclic combinatorial objects, *Discrete Math.* **197/198** (1999), 589–606.
- [12] M. Muzychuk, A solution of the isomorphism problem for circulant graphs, *London Math. Soc.* (3) **88** (2004), 1–41.
- [13] H. Qu and J. Yu, On isomorphism of Cayley digraphs on dihedral groups, *Australian J. Combin.* **15** (1997), 213–220.
- [14] P. Spiga, On the Cayley isomorphism problem for a digraph with 24 vertices, *Ars Math. Contemp.* **1** (2008), 38–43.

- [15] L. Sun, Isomorphisms of circulants with degree 2, *J. Beijing Ins. Technol.* **9** (1984), 42–46.
- [16] D. Wiedemann and M. E. Zieve, Equivalence of sparse circulants: the bipartite Ádám problem, preprint arXiv:0706.1567v1 [math. CO] (2007).
- [17] S. J. Xu, W. Jin, Q. Shi, J. J. Li, The BCI-property of the Bi-Cayley graphs, *J. Guangxi Norm. Univ.: Nat. Sci. Edition* **26** (2008), 33–36.